Claims

[c1] 1. A method for a first user to provide secure access to electronic documents or services stored on a document server located on a network to a second user, where the first user is a registered user of the document server and the second user is not a registered user of the document server, and where both the first user, the second user, and the document server have each associated therewith a public key that is associated with a corresponding private key, the method performed on the document server comprising:

exchanging public keys with the first user to establish a first secure session;

receiving from the first user a request to list a file directory; authenticating the first user's access to the file directory using credentials provided by the first user when the first secure session is established;

transmitting to the first user a listing of the file directory over the first secure session; the listing identifying a set of paths to content available on the document server;

exchanging public keys with the second user to establish a second secure session;

receiving from the second user a request for access to selected content on the document server; the request for access including a token identifier that is recorded at the document server and associated with a path from the set of paths to the selected content available on the document server;

authenticating the request for access using: (a) the public key of the second user received from the second user while establishing the second secure session, and (b) a digital signature signed using the private key of the first user that is a signed cryptographic digest of the public key of the second user and other information relating to the request for access to the selected document content on the document server; and

providing the second user with access to the selected content over the second secure session if the request for access is authenticated.

[c2] 2. The method according to claim 1, further comprising:

receiving from the first user a request to create a token that is associated with the path to the selected content available on the document server;

creating the token in a database of tokens on the document server; the token having associated therewith the token identifier; and
transmitting to the first user over a secure session the token identifier that uniquely identifies the token in the token database.

[c3] 3. The method according to claim 2, further comprising:
receiving from the first user over the first secure session the path from the set of paths identifying selected content available on the document server;
transmitting to the first user the token identifier over the first secure session; the token identifier being associated with the path to the selected content available on the document server; and
receiving from the first user over the first secure session the digital signature of the signed cryptographic digest of the public key of the second user and the token identifier.

[c4] 4. The method according to claim 3, wherein each public key forms part of a digital certificate.

[c5] 5. The method according to claim 3, further comprising receiving over a third secure session a request from the first user to modify access rights recorded with the token in the token database.

[c6] 6. The method according to claim 2, receiving from the first user over a third secure session the digital signature of the signed cryptographic digest of the public key of the second user and the other information relating to the request for access to the selected document content on the document server.

[c7] 7. The method according to claim 2, wherein the digital signature signed by the private key of the first user is received with the request for access to the selected content available on the document server from the second user.

[c8] 8. The method according to claim 2, wherein the cryptographic digest signed using the private key of the first user includes a cryptographic digest of all or portions of the selected content.

[c9] 9. The method according to claim 2, wherein the other information relating to

the request for access to the selected document content on the document server includes one or more of the token identifier, a creation date of the token, access rights to the selected content, all or portions of the selected content, and a version number of the selected content.

[c10] 10. The method according to claim 1, wherein the request for access is specified using a secure hypertext transfer protocol that includes a gateway address, the digital signature, and the path of the selected content available on the document server.

[c11] 11. The method according to claim 1, wherein the document server is located on an intranet protected by a firewall and wherein the first secure session and the second secure session tunnel through the firewall.

[c12] 12. The method according to claim 1, wherein the other information relating to the request for access to the selected document content on the document server is one of the token identifier, the path from the set of paths to the selected content available on the document server, and access rights to the selected document content, and wherein the selected content is one of a document and a service available on the document server.

[c13] 13. An article of manufacture for use in a machine, comprising:
a memory;
instructions stored in the memory for a method in which a first user provides secure access to electronic documents or services stored on a document server located on a network to a second user, where the first user is a registered user of the document server and the second user is not a registered user of the document server, and where both the first user, the second user, and the document server have each associated therewith a public key that is associated with a corresponding private key, the method comprising:
exchanging public keys with the first user to establish a first secure session;
receiving from the first user a request to list a file directory; authenticating the first user's access to the file directory using credentials provided by the first user when the first secure session is established;
transmitting to the first user a listing of the file directory over the first secure

session; the listing identifying a set of paths to content available on the document server;

exchanging public keys with the second user to establish a second secure session;

receiving from the second user a request for access to selected content on the document server; the request for access including a token identifier that is recorded at the document server and associated with a path from the set of paths to the selected content available on the document server;

authenticating the request for access using: (a) the public key of the second user received from the second user while establishing the second secure session, and (b) a digital signature signed using the private key of the first user that is a signed cryptographic digest of the public key of the second user and other information relating to the request for access to the selected document content on the document server; and

providing the second user with access to the selected content over the second secure session if the request for access is authenticated.

[c14] 14. The article of manufacture according to claim 13, wherein the method further comprises:

receiving from the first user a request to create a token that is associated with the path to the selected content available on the document server;

creating the token in a database of tokens on the document server; the token having associated therewith the token identifier; and

transmitting to the first user over a secure session the token identifier that uniquely identifies the token in the token database.

[c15] 15. The article of manufacture according to claim 14, wherein the method further comprises:

receiving from the first user over the first secure session the path from the set of paths identifying selected content available on the document server;

transmitting to the first user the token identifier over the first secure session; the token identifier being associated with the path to the selected content available on the document server; and

receiving from the first user over the first secure session the digital signature of

the signed cryptographic digest of the public key of the second user and the token identifier.

[c16] 16. The article of manufacture according to claim 13, wherein the other information relating to the request for access to the selected document content on the document server is one of the token identifier, the path from the set of paths to the selected content available on the document server, and access rights to the selected document content, and wherein the selected content is one of a document and a service available on the document server.

[c17] 17. A document server for performing a method in which a first user provides secure access to electronic documents or services stored on the document server located on a network to a second user, where the first user is a registered user of the document server and the second user is not a registered user of the document server, and where both the first user, the second user, and the document server have each associated therewith a public key that is associated with a corresponding private key, the document server comprising:
a memory for storing instructions; and
a processor coupled to the memory for executing the instructions of the document server; the processor in executing the instructions:
exchanging public keys with the first user to establish a first secure session;
receiving from the first user a request to list a file directory; authenticating the first user's access to the file directory using credentials provided by the first user when the first secure session is established;
transmitting to the first user a listing of the file directory over the first secure session; the listing identifying a set of paths to content available on the document server;
exchanging public keys with the second user to establish a second secure session;
receiving from the second user a request for access to selected content on the document server; the request for access including a token identifier that is recorded at the document server and associated with a path from the set of paths to the selected content available on the document server;
authenticating the request for access using: (a) the public key of the second

user received from the second user while establishing the second secure session, and (b) a digital signature signed using the private key of the first user that is a signed cryptographic digest of the public key of the second user and other information relating to the request for access to the selected document content on the document server; and
providing the second user with access to the selected content over the second secure session if the request for access is authenticated.

[c18] 18. The document server according to claim 17, wherein the processor in executing the instructions executes instructions for:
receiving from the first user a request to create a token that is associated with the path to the selected content available on the document server;
creating the token in a database of tokens on the document server; the token having associated therewith the token identifier; and
transmitting to the first user over a secure session the token identifier that uniquely identifies the token in the token database.

[c19] 19. The method according to claim 18, wherein the processor in executing the instructions executes instructions for:
receiving from the first user over the first secure session the path from the set of paths identifying selected content available on the document server;
transmitting to the first user the token identifier over the first secure session; the token identifier being associated with the path to the selected content available on the document server; and
receiving from the first user over the first secure session the digital signature of the signed cryptographic digest of the public key of the second user and the token identifier.

[c20] 20. The method according to claim 17, wherein the other information relating to the request for access to the selected document content on the document server is one of the token identifier, the path from the set of paths to the selected content available on the document server, and access rights to the selected document content, and wherein the selected content is one of a document and a service available on the document server.